Principles of Cryptography Problem Sheet 4

Dr. Kurunandan Jain[1]†,

[1]Department of Mathematics, Amrita Vishwa, Amrita Campus, Kollam-690525, Kerala, India

(Received xx; revised xx; accepted xx)

1) Understanding the functionality of groups, and cyclic groups is important for the use of public key cryptosystems based on the discrete logarithm problem. That's why we are going to practice some arithmetic in such structures in this set of problems

Let's start with an easy one. Determine the order of all elements of the multiplicative group of:

a) $\mathbb{Z}_5^*$

b) $\mathbb{Z}_7^*$

c) $\mathbb{Z}_{13}^*$

2) We now study the groups from the above Problem

a) How many elements does each of the multiplicative groups have?

b) Do all orders from above divide the number of elements in the corresponding multiplicative group?

c) Which of the elements are primitive elements?

d) Verify for the group that the number of primitive elements is given by $\phi(|\mathbb{Z}_p^*|)$

3) Compute the two public keys and the common key for DHKE scheme with the parameters $p = 467$ and $\alpha = 2$ and

a) $a = 3$ and $b = 5$

b) $a = 400$ and $b = 134$

c) $a = 228$ and $b = 57$

4) In DHKE protocol, the private keys are chosen from the set $[2, \cdots p-2]$

Why are the values 1 and $p-1$ excluded? Describe the weakness of these two values

5) Encrypt the following messages with the Elgamal scheme $p = 467$ and $\alpha = 2$

a) $k_{pr} = d = 105$ and $i = 213$ and $x = 33$

b) $k_{pr} = d = 105$ and $i = 123$ and $x = 33$

c) $k_{pr} = d = 300$ and $i = 45$ and $x = 248$

d) $k_{pr} = d = 300$ and $i = 47$ and $x = 248$

6) Show that the condition $4a^3 + 27b^2 \neq 0 \mod p$ is fulfilled for the curve $y^2 \equiv x^3 + 2x + 2 \mod 17$

b) Perform the additions (2,7)+(5,2) and (3,6)+(3,6)

7) Verify Hasse's theorem for the the above curve knowing $\#E = 19$

8) Let E be an elliptic curve defined over $\mathbb{Z}_7 : y^2 = x^3 + 3x + 2$

a) Compute all the points on E over $\mathbb{Z}_7$

b) What is the order of the group?

c) Given the element $\alpha = (0, 3)$ determine the order of α. Is α a primitive element?

9) Give an elliptic curve E over $\mathbb{Z}_{29}$ and the base point $P = (8, 10)$: E: $y^2 = x^3 + 4x + 20$

Calculate the following point multiplication using the Double and add algorithm, provide the steps

a) $k = 9$

b) $k = 20$

† Email address for correspondence: kurunandanj@am.amrita.edu

10) Your task is to compute a session key in a DHKE protocol based on elliptic curves. Your private key is $a = 6$. You receive Bob's public key $B = (5, 9)$. The elliptic curve being used is defined by $y^2 \equiv x^3 + x + 6 \mod 11$